AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions, and listings, of claims in this application:

1. (Currently Amended) A method for generating a repeatable cryptographic key using at least one parameter comprising the steps of:

generating at least one index as a function of said at least one parameter, said one parameter being from a plurality of varying parameters;

retrieving at least one cryptographic share from a memory location identified as a function of said at least one index; and

generating ~~a~~ said repeatable cryptographic key based on said at least one cryptographic share, wherein said generated repeatable cryptographic key remains the same from one said generating of said repeatable cryptographic key to a next generating of said repeatable cryptographic key regardless of whether said plurality of varying parameters change from said generating of said repeatable cryptographic key to said next generating of said repeatable cryptographic key.

2. (Original) The method of claim 1 wherein said at least one retrieved cryptographic share is encrypted, said method further comprising the step of:

decrypting said at least one cryptographic share.

3. (Original) The method of claim 2 wherein said step of decrypting comprises the step of:

decrypting using a value computed as a function of said at least one parameter.

4. (Cancelled).

5. (Cancelled).

6. (Original) The method of claim 1 wherein said at least one parameter represents at least one measurement of a physical property.

7. (Currently Amended) The method of claim 1 wherein the plurality of varying parameters change from ~~one~~ said one generation of said repeatable cryptographic key to ~~a~~ said next generation of ~~said~~ said repeatable cryptographic key.

8. (Original) The method of claim 7 further comprising the step of:

retrieving a cryptographic share from a memory location in the vicinity of said memory location identified by said index.

9. (Original) The method of claim 7 wherein said step of generating at least one index comprises the step of generating the same index for a set of parameter values.

10. (Original) The method of claim 9 wherein said set of parameter values are within a predetermined range of values.

Claims 11 through 23 (Previously Cancelled).

24. (Currently Amended) A method for generating a repeatable cryptographic key comprising the steps of:

measuring a plurality of keystroke features during entry of a password;

generating a plurality of indices using said plurality of keystroke features;

retrieving from a data structure a plurality of cryptographic shares as a function of said plurality of indices; and

generating ~~a~~ said repeatable cryptographic key using said cryptographic shares wherein said generated repeatable cryptographic key remains the same from one said generating of said repeatable cryptographic key to a next generating of said repeatable cryptographic key regardless of whether said plurality of keystroke features change from said one generating of said cryptographic repeatable key to said next generating of said repeatable cryptographic key.

25. (Original) The method of claim 24 wherein said cryptographic shares represent points on a polynomial.

26. (Original) The method of claim 24 wherein said cryptographic shares represent vectors.

27. (Original) The method of claim 24 wherein said cryptographic shares are compressed.

28. (Original) The method of claim 27 wherein said cryptographic shares comprise y values of points on a polynomial and the corresponding x values are derivable from a data structure location.

29. (Currently Amended) The method of claim 24 wherein said plurality of keystroke features vary from said one generating of said repeatable cryptographic key to ~~a~~ said next generation of said repeatable cryptographic key

30. (Previously Amended) The method of claim 24 wherein said step of generating a plurality of indices as a function of said keystroke features comprises the step of:

for each of said keystroke features, generating one of two indices as a function of a threshold value, h_i, where said function is defined by:

$$f(\phi_1,\phi_2,...\phi_m)=\{\psi_1,\psi_2,...\psi_m\}\in\{0,1\}^m$$

where

ϕ represents said keystroke features, ψ represents said indices, m is a particular number of measured features associated with said password; and

$$\psi_i\begin{cases}0 \text{ if } \phi_i < h_i\\ 1 \text{ if } \phi_i \geq h_i\end{cases}.$$

31. (Previously Amended) The method of claim 24 wherein said step of generating a plurality of indices as a function of said keystroke features comprises the step of:

for each of said keystroke features, generating one of a plurality of indices as a function of a plurality of threshold values, h_i, where said function is defined by:

$$f(\phi_1,\phi_2,...\phi_m)=\{\psi_1,\psi_2,...\psi_m\}\in\{0,1\}^m$$

where

ϕ represents said keystroke features, ψ represents said indices, m is a particular number of measured features associated with said password; and

$$\psi_i\begin{cases}0 \text{ if } \phi_i < h_i\\ 1 \text{ if } \phi_i \geq h_i\end{cases}.$$

32. (Original) The method of claim 24 wherein said cryptographic shares stored in said data structure are encrypted, said method further comprising the step of:

decrypting said cryptographic shares using said password.

33. (Original) The method of claim 24 further comprising the steps of:

maintaining a history file containing information relating to prior successful key generation attempts; and

based on said history file, storing invalid cryptographic shares in data structure locations which are not expected to be accessed during subsequent legitimate key generation attempts.

34. (Currently Amended) A method for generating a repeatable cryptographic key using a plurality of varying parameters, said varying parameters representing physical measurements, said method comprising the steps of:

for each of said plurality of parameters:

generating at least one index using said parameter;

retrieving an encrypted cryptographic share from a memory location as a function of said at least one index;

decrypting said encrypted cryptographic share with a function of said parameter; and

generating ~~a~~ said repeatable cryptographic key using said decrypted cryptographic shares, wherein said generated repeatable cryptographic key remains the same from one said generating of said repeatable cryptographic key to a next generating of said repeatable cryptographic key regardless of whether said plurality of varying parameters change from said one generating of said repeatable cryptographic key to said next generating of said repeatable cryptographic key.

35. (Original) The method of claim 34 wherein said physical measurements are measurements of DNA.

36. (Original) The method of claim 34 wherein said function of said parameter used to decrypt said encrypted cryptographic share is a hash function.

37. (Currently Amended) A data structure for use in generating a repeatable cryptographic key based on *n* parameters representing physical measurements, said data structure comprising:

n storage locations each associated with a respective one of said *n* parameters, each particular storage location containing an encrypted cryptographic share which was encrypted using an expected value of a function of the parameter associated with said particular storage location, each said *n* storage location being associated with at least one index of a plurality of indices, where said plurality of indices are generated using said physical measurements such that said repeatable cryptographic key remains the same from one generation to a next generation of said repeatable cryptographic key regardless of whether said *n* parameters change from said one generation of said repeatable cryptographic key to said next generation of said repeatable cryptographic key.

38. (Original) The data structure of claim 37 wherein said function is a hash function.

39. (Currently Amended) The data structure of claim 37 wherein said repeatable cryptographic key may be generated using less than *n* cryptographic shares.